Galois characteristics of local fields

These are the notes of the talk I gave at the University of Copenhagen on 9th December 2016.

The main question of this talk is what information about a field can be deduced from its absolute Galois group.

Let us have a look at two examples: For number fields, the theorem of Neukirch-Uchida tells us that two number fields are isomorphic if and only if their absolute Galois groups are. There are similar results for other types of fields as well, for example for finitely generated fields.

On the other hand, every finite field has absolute Galois group isomorphic to $\hat{\mathbb{Z}}$, so in this case when can deduce no information whatsoever from it, not even the characteristic of the field.

The study of these phenomena is called *Anabelian Geometry*. We will not explain the geometry bit (the words scheme or fundamental group will not be used in this article). The general philosophy, however, is that if a group (here the absolute Galois group) is attached to a certain object (here a field), then one should be able to recover information about the object from the group as long as the group is 'sufficiently non-abelian'.

Let us look at finite extensions K of $\mathbb{Q}_p$: Here one knows (Jarden-Ritter) that there are non-isomorphic fields with isomorphic Galois groups. This follows, at least morally[1], from a theorem by Jannsen-Wingberg determining explicitly the absolute Galois group of K in terms of (profinite) generators and relations. It is then not hard to come up with two non-isomorphic fields having the same generators and relations, and the examples they give are completely explicit.

Nonetheless, Mochizuki showed that if the absolute Galois group is given *together with all its ramification subgroups* (in the upper numbering), then the field is uniquely determined by this data. The purpose of this article is to talk about the methods involved in Mochizuki's proof, focussing on the use of a certain Hodge-Tate representation coming from Lubin-Tate theory.

1 Precise question

Fix a prime number p, a finite extension $K|\mathbb{Q}_p$, an algebraic closure $\overline{K}$, and let us denote the absolute Galois group of K by $G_K := \mathrm{Gal}(\overline{K}|K)$.

Let us first have a look at what happens if a field isomorphism $\alpha\colon K \xrightarrow{\sim} K'$ is given. We can extend α to an isomorphism $\overline{\alpha}$ between the algebraic closures such that the following diagram commutes

[1]This is chronologically incorrect. Jannsen-Wingberg came after Jarden-Ritter.

$$\begin{array}{ccc} \overline{K} & \xrightarrow{\overline{\alpha}} & \overline{K'} \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i'} \\ K & \xrightarrow[\alpha]{\sim} & K'. \end{array}$$

Here i and i' denote (for now fixed) embeddings of K and K' into their algebraic closures.

This now induces a continuous isomorphism between the absolute Galois groups

$$\Phi(\overline{\alpha})\colon G_K \xrightarrow{\sim} G_{K'}, \quad \sigma \mapsto \overline{\alpha} \circ \sigma \circ \overline{\alpha}^{-1}$$

which defines a homomorphism

$$\Phi\colon \operatorname{Isom}\Big(\big(\overline{K}|K\big), \big(\overline{K'}|K'\big)\Big) \to \operatorname{Isom}(G_K, G_{K'}), \quad (\overline{\alpha}, \alpha) \mapsto \Phi(\overline{\alpha}),$$

where the left hand side is the set of all pairs $(\overline{\alpha}, \alpha)$ of isomorphisms $\overline{\alpha}\colon \overline{K} \xrightarrow{\sim} \overline{K'}$ and $\alpha\colon K \xrightarrow{\sim} K'$ for which the above diagram commutes, and the right hand side is the set of all continuous group isomorphisms from G_K to $G_{K'}$.

The precise statement of the Neukirch-Uchida theorem is that for number fields K,K', this map Φ is an isomorphism. For other types of fields, Φ is injective, but in general not surjective. For example, for p-adic local fields $K|\mathbb{Q}_p$ it is not surjective.

Mochizuki's idea is to replace $\operatorname{Isom}(G_K, G_{K'})$ by $\operatorname{Isom}_{\text{filt}}(G_K, G_{K'})$, the subset of all isomorphisms preserving the filtration given by the ramification subgroups. In order to show surjectivity, he needs to construct a field isomorphism $\alpha(\varphi)\colon K \xrightarrow{\sim} K'$ from a given isomorphism of filtered groups $\varphi \in \operatorname{Isom}_{\text{filt}}(G_K, G_{K'})$, such that $\Phi(\overline{\alpha}) = \varphi$ (where $\overline{\alpha}$ is a (suitably constructed) extension of α to $\overline{K}$).

The strategy of this construction is a step-by-step, group-theoretical recovery of certain objects attached to K, e.g. the numbers q_K and $[K : \mathbb{Q}_p]$ or the G_K-module $\mu(\overline{K})$, first from the Galois group G_K alone, later from G_K and its ramification subgroups G_K^u. These recoveries allow one to determine the Hodge-Tate numbers of a given representation of G_K entirely group-theoretically. Applying this to (a variant of) the Lubin-Tate representation of G_K, one is able to construct the required field isomorphism.

Schematic picture

2 Recap Local Class Field Theory

2.1 Theorem. *There exists exactly one family of continuous homomorphisms*

$$\operatorname{rec}_K\colon K^\times \to G_K^{\text{ab}},$$

the reciprocity maps, with the following properties:

1. *The composite* $K^\times \to G_K^{\text{ab}} \to \operatorname{Gal}(K^{\text{nr}}|K)$, $x \mapsto \operatorname{rec}_K(x)|_{K^{\text{nr}}}$ *is given by* $x \mapsto \operatorname{Fr}^{v_K(x)}$.

2. *For a finite extension $L|K$, i.e. for an open subgroup $G_L \subset G_K$, we get two commutative diagrams*

$$\begin{array}{ccc} L^\times & \xrightarrow{\mathrm{rec}_L} & G_L^{\mathrm{ab}} \\ {\scriptstyle N_{L|K}}\downarrow & & \downarrow \\ K^\times & \xrightarrow[\mathrm{rec}_K]{} & G_K^{\mathrm{ab}} \end{array} \tag{2.1}$$

and

$$\begin{array}{ccc} L^\times & \xrightarrow{\mathrm{rec}_L} & G_L^{\mathrm{ab}} \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ K^\times & \xrightarrow[\mathrm{rec}_K]{} & G_K^{\mathrm{ab}}. \end{array} \tag{2.2}$$

Here Fr is the arithmetic Frobenius in $\mathrm{Gal}(K^{\mathrm{nr}}|K)$ and Ver is the 'Verlagerung' or transfer map, a completely group-theoretical construction between the abelianisation of a group and the abelianisation of a subgroup of finite index.

We will also need some additional properties of the reciprocity maps which will be pointed out later.

3 Reconstructions from the absolute Galois group

We will start our sequence of group-theoretical recoveries from G_K with the following lemma. (Footnote that we won't define what a recovery actually is)

3.1 Lemma (Recovery of the G_K-module of roots of unity)**.** *The G_K-module $\mu(\overline{K})$ of roots of unity can be recovered group-theoretically from G_K.*

Proof. Local Class Field Theory gives the following short exact sequence of abelian groups (Footnote: I did not mention the injectivity or the image of rec_K - give them here as a footnote)

$$0 \longrightarrow K^\times \xrightarrow{\mathrm{rec}_K} G_K^{\mathrm{ab}} \longrightarrow \hat{\mathbb{Z}}/\mathbb{Z} \longrightarrow 0.$$

Looking at the torsion subgroups, and using the fact that $\hat{\mathbb{Z}}/\mathbb{Z}$ is uniquely divisible (use the snake lemma) and hence torsion free, yields

$$\mu(K) \cong \left(G_K^{\mathrm{ab}}\right)_{\mathrm{tors}}$$

as abelian groups. Since the right hand side is determined entirely by group-theoretical constructions applied to G_K, we can recover the abelian group $\mu(K)$.

In the same way we get, for a finite Galois extension $L|K$, an isomorphism

$$\mathrm{rec}_L \colon \mu(L) \xrightarrow{\sim} \left(G_L^{\mathrm{ab}}\right)_{\mathrm{tors}}$$

not only as abelian groups, but as $\mathrm{Gal}(L|K)$-modules, as rec_L is $\mathrm{Gal}(L|K)$-equivariant. Hence we can recover the $\mathrm{Gal}(L|K)$-module $\mu(L)$.

In order to recover

$$\mu(\overline{K}) = \varinjlim_{L} \mu(L),$$

we still need to recover the transition maps $\mu(L) \to \mu(L')$, but these can be recovered using the Verlagerung (2.2). □

3.2 Corollary (Recovery of the cyclotomic character)**.** *The (p-)cyclotomic character*

$$\chi\colon G_K \to \mathbb{Z}_p^\times$$

can be recovered group-theoretically from G_K.

Proof. We look at the subgroup $\mu_{p^\infty}(\overline{K})$ of roots of unity of p-power order. As this is constructed purely group-theoretically from $\mu(\overline{K})$, we can recover this G_K-module using the preceding lemma. Now by definition of the cyclotomic character

$$s(\zeta) = \zeta^{\chi(s)}, \quad s \in G_K,\ \zeta \in \mu_{p^\infty}(\overline{K}),$$

i.e. χ precisely encodes the G_K-action on p-power-order roots of unity, so its recovery is the same as the recovery of the G_K-module $\mu_{p^\infty}(\overline{K})$. □

Using similar techniques, one can continue to recover the order q_K of the residue field and the degree $[K : \mathbb{Q}_p]$, hence also ramification indices and residue degrees. Thus one can recover the inertia subgroup I_K and (by reciprocity) the abelian group U_K of units in K.

Now let us assume that not only G_K, but also all ramification subgroups $(G_K^u)_{u\geq -1}$ are given – this corresponds to $\varphi \in \mathrm{Isom}(G_K, G_{K'})$ preserving the ramification subgroups. Using exactly the same techniques (i.e. Local Class Field Theory) and the p-adic logarithm one gets the following lemma.

3.3 Lemma (Recovery of $\mathbb{C}_p$)**.** *The G_K-module $\mathbb{C}_p$ can be recovered group-theoretically from $(G_K, (G_K^u)_{u\geq -1})$.*

4 Hodge-Tate representations

4.1 Definition. *Let W be a finite dimensional $\mathbb{C}_p$-vector space equipped with a semi-linear G_K-action, i.e.*

$$s(c \cdot w) = s(c) \cdot s(w), \quad s \in G_K,\ c \in \mathbb{C}_p,\ w \in W.$$

For $i \in \mathbb{Z}$ define the K-vector spaces

$$W^i := \{w \in W \mid s(w) = \chi(s)^i w \text{ for all } s \in G_K\}$$

and the $\mathbb{C}_p$-vector spaces

$$W(i) := \mathbb{C}_p \otimes_K W^i.$$

Define the Hodge-Tate numbers of W by

$$d_W(i) := \dim_K W^i = \dim_{\mathbb{C}_p} W(i), \quad i \in \mathbb{Z}.$$

It is a fact (due to Tate) that $\bigoplus_{i\in\mathbb{Z}} W(i)$ injects into W, hence the $W(i)$ are finite dimensional and the numbers $d_W(i)$ are defined.

4.2 Definition. *Call W a Hodge-Tate module if this injection is an isomorphism, i.e. if*

$$\sum_{i\in\mathbb{Z}} d_W(i) = \dim_{\mathbb{C}_p} W.$$

As we have already recovered both the G_K-action on $\mathbb{C}_p$ and the cyclotomic character χ from the filtered absolute Galois group, and this is all that is involved in the definition of the Hodge-Tate numbers, we can conclude:

4.3 Lemma. *Given W as above. Then one can group-theoretically recover the Hodge-Tate numbers of W from $(G_K, (G_K^u)_{u\geq -1})$ (and W).*

4.4 Example. Define $\mathbb{C}_p(\chi^i)$ to be a 1-dimensional $\mathbb{C}_p$-vector space (with basis vector b, say), where the usual Galois action of G_K on $\mathbb{C}_p$ is twisted by the i-th power of the cyclotomic character χ:

$$s(c \cdot b) := \chi^i(s)s(c) \cdot b, \quad s \in G_K,\ c \in \mathbb{C}_p.$$

From the definition of the Hodge-Tate numbers follows

$$d_{\mathbb{C}_p(\chi^i)}(i) = 1, \quad d_{\mathbb{C}_p(\chi^i)}(j) = 0,\ j \neq i.$$

Hence for any W, being a Hodge-Tate module means there is an isomorphism of $\mathbb{C}_p$-vector spaces

$$W \cong \bigoplus_{i\in\mathbb{Z}} \mathbb{C}_p(\chi^i)^{d_W(i)}$$

respecting the G_K-action. Thus one should think of Hodge-Tate modules as those representations of G_K on $\mathbb{C}_p$-vector spaces which allow such a decomposition into "eigenspaces" with "eigenvalues" equal to powers of the cyclotomic character – quite similar to representations of finite groups, for example.

It will be convenient to talk about a representation of G_K on vector spaces over fields smaller than $\mathbb{C}_p$ and also define their Hodge-Tate numbers.

4.5 Definition. *A representation (in this article) will always be a continuous group homomorphism*

$$\rho\colon G_K \to M^\times,$$

where M is some finite extension of $\mathbb{Q}_p$ equipped with its p-adic topology.

Now take a 1-dimensional vector space V over M and let G_K act on V via ρ. Define the $\mathbb{C}_p$-vector space

$$W := \mathbb{C}_p \otimes_{\mathbb{Q}_p} V$$

and equip it with the obvious semi-linear Galois action

$$s(c \otimes v) := s(c) \otimes \rho(s)v, \quad s \in G_K, c \in \mathbb{C}_p, v \in V.$$

Now the Hodge-Tate numbers of W are also called the Hodge-Tate numbers of V and we use the notation $d_V(i) := d_W(i)$. Moreover we call V and ρ a Hodge-Tate representation, if W is a Hodge-Tate module.

The crucial example of a Hodge-Tate representation is the following representation obtained by Lubin-Tate theory – hence we will call it the Lubin-Tate representation.

4.6 Definition. *Let $\pi \in K$ be a uniformizer. The Lubin-Tate representation of G_K is*

$$\rho_{\mathrm{LT}} \colon G_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}|K) \longrightarrow \mathrm{Gal}(K_\pi|K) \xrightarrow{\sim} U_K \longrightarrow U_K \subset K^\times \tag{4.1}$$

$$s \longmapsto s|_{K^{\mathrm{ab}}} \longmapsto s|_{K_\pi} = (u, K_\pi|K) \longmapsto u \longmapsto u^{-1}.$$

Here, K_π is an infinite, totally ramified extension of K which is explicitly constructed by Lubin-Tate theory, attaching torsion points of a certain formal group to K. The isomorphism $\mathrm{Gal}(K_\pi|K) \xrightarrow{\sim} U_K$ comes from the reciprocity map of local class field theory. One composes with the inversion $u \mapsto u^{-1}$ as the explicit action of U_K on the torsion points of the formal group is given that way.

It is very important to note that on the inertia subgroup I_K, under the reciprocity map $\mathrm{rec}_K \colon U_K \xrightarrow{\sim} I_K$, the Lubin-Tate representation ρ_{LT} looks like $u \mapsto u^{-1}$. This specific shape on the inertia subgroup is crucial for Hodge-Tate representations – that is what Serre's result on Hodge-Tate representations being locally algebraic is about.

Let's start the discussion of (a variant of) Serre's result by calculating the Hodge-Tate numbers of the Lubin-Tate representation. So let V_π be a 1-dimensional K-vector space on which G_K acts via ρ_{LT}.

4.7 Proposition. *The Lubin-Tate representation ρ_{LT}, acting on the 1-dimensional K-vector space V_π, has the Hodge-Tate numbers*

$$d_{V_\pi}(0) = [K : \mathbb{Q}_p] - 1,$$
$$d_{V_\pi}(1) = 1.$$

In particular, it is a Hodge-Tate representation.

Proof. Tate "p-divisible groups", §4, Cor. 2 to Thm. 3. Tate uses the language of p-divisible groups which might look frightening, but the translation into the language of formal groups is not too hard. A detailed dictionary can be found in my thesis. □

We now state the variant of Serre's result which we will need, and give some idea how one can deduce it from Serre's original result.

4.8 Theorem. *Let $F|\mathbb{Q}_p$ be a finite Galois extension with $K \subset F$, and let $\rho\colon G_K \to F^\times$ be a representation with associated 1-dimensional F-vector space V.*

Then V has the Hodge-Tate numbers

$$d_V(0) = [F : K]\big([K : \mathbb{Q}_p] - 1\big),$$
$$d_V(1) = [F : K]$$

if and only if there exists a field embedding $\iota\colon K \hookrightarrow F$ and an open subgroup $I \subset U_K$ such that

$$\rho \circ \mathrm{rec}_K\,|_I = \iota \circ (\cdot)^{-1}\colon I \to U_F.$$

4.9 Remark.

1. Where do the above Hodge-Tate numbers come from? They are $[F : K]$ times the Hodge-Tate numbers of the Lubin-Tate representation! An easy calculation shows that these are the Hodge-Tate numbers of the Lubin-Tate representation composed with the inclusion $K \hookrightarrow F$.

2. The main input in proving theorem 4.8 is Serre's result about Hodge-Tate representations being 'locally algebraic' (Serre "Abelian l-adic representations and elliptic curves", Ch. III, appendix, §5, Cor. to Thm. 2). This roughly states that the shape of a Hodge-Tate representation on an open subgroup of the inertia subgroup is very similar to the shape of the Lubin-Tate representation, so (reciprocity composed with) inversion.

   However, Serre's situation is somewhat different – for example, he looks at representations $\rho\colon G_K \to E^\times$ with $E \subset K$, whereas here $\rho\colon G_K \to F^\times$ with $K \subset F$.

3. In order to deduce theorem 4.8 from Serre's result, one needs to do some calculations about the effect of changing the fields (from K to F, for example). It is a little subtle, but doable, and again the details can be found in my thesis.

5 Construction of the field isomorphism

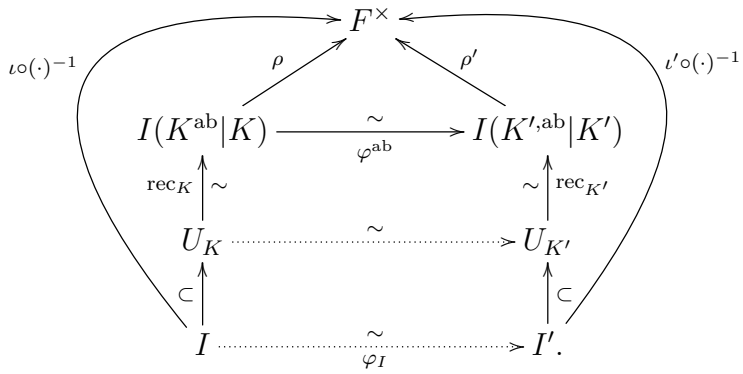
We are finally ready to construct the desired field isomorphism. Given two finite extensions K, K' of $\mathbb{Q}_p$ and $\varphi \in \mathrm{Isom}_{\mathrm{filt}}(G_K, G_{K'})$. Now choose a finite Galois extension $F|\mathbb{Q}_p$ with $K, K' \subset F$, and choose a representation $\rho\colon G_K \to F^\times$ with Hodge-Tate numbers as in theorem 4.8 – for example, take the Lubin-Tate representation of K and compose it with $K \hookrightarrow F$.

Since we have recovered the Hodge-Tate numbers of a representation, we know that the representation

$$\rho' := \rho \circ \varphi^{-1}\colon G_{K'} \to F^\times$$

has the same Hodge-Tate numbers as ρ, but is (of course) a representation of the absolute Galois group of K'.

Now by theorem 4.8, there exists open subgroups $I \subset U_K$ and $I' \subset U_{K'}$ and field embeddings $\iota\colon K \hookrightarrow F$ and $\iota'\colon K' \hookrightarrow F$ such that we get the following commutative diagram



(5.1)

(All horizontal arrows are induced by φ. If necessary, shrink I or I' to make the last horizontal arrow into an isomorphism.)

Thus viewing I and I' via ι and ι' as subsets of F, they are exactly identified via φ_I. By $\mathbb{Q}_p$-linear continuation of φ_I and using $K = \mathrm{span}_{\mathbb{Q}_p} I$, we get a field isomorphism

$$\alpha(\varphi)\colon K \xrightarrow{\sim} K'.$$

By doing the same procedure on an open subgroup G_L of G_K, we also get field isomorphisms $L \xrightarrow{\sim} L'$, and one can show that these construction are compatible, hence we get a field isomorphism

$$\overline{\alpha}(\varphi)\colon \overline{K} \xrightarrow{\sim} \overline{K'}.$$

5.1 Remark. It remains to show that this isomorphism $\overline{\alpha}(\varphi)$ actually induces the group isomorphism φ we started with, i.e. that $\Phi(\overline{\alpha}(\varphi)) = \varphi$. This is actually a little tricky and more details can be found in my thesis.